Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
	)	
To: The Commission	)	

WRITTEN EX PARTE COMMENTS OF ZipDX LLC

Submitted to the Record

David Frankel
dfrankel@zipdx.com
17554 Via Sereno
Monte Sereno, CA 95030
Tel: 800-372-6535

Filed: August 4, 2017

Having reviewed the Reply Comments (and earlier Comments) responding to the Commission's NPRM and NOI FCC 17-24, ZipDX submits this document.

NPRM: Provider blocking of DNO and "Invalid" Numbers

The bulk of the commenters generally support the NPRM. In their Reply Comments, USTelecom states: "Multiple commenters from a broad range of industries and a diversity of interests, expressed strong support for permitting such blocking of the four categories of calls identified by the Commission in its Notice."[1] They continue: "Very few commenters express outright opposition to the Commission's proposal, although some note that adoption of the Commission's proposal would not capture large volumes of calls."[2]

According to USTelecom: "The Commission should not let the perfect be the enemy of the good…."[3] A key factor in the applicability of this common aphorism, which we sometimes use ourselves, is whether or not the matter under consideration is in fact "good."

Regrettably, this NPRM is not "good". It suffers from several severe and unfixable defects:

1) It will block a statistically insignificant number of illegal robocalls.
2) It is trivial for robocallers to work around.
3) It will ensnare large numbers of legitimate calls.

We explained this in our Comments and a few others also made mention of one or more of these three points. No Reply Comments rebutted our position.

[1] Reply Comments of The USTelecom Association, page 2 (available at https://ecfsapi.fcc.gov/file/10731798828512/USTelecom-Blocking-Reply-Comments-2016-07-31-FINAL.pdf)
[2] Ibid, page 2
[3] Ibid, page 2

In fact, amazingly, the Reply Comments are generally devoid of any real data. It is disappointing that despite having access to billions of actual call records, none of the service providers or industry associations that are participating in this docket could lift a finger to definitively examine how the proposed call filters would behave in the context of actual telephone calls. There is only some speculation on what might or might not happen and generalizations on what could or should happen.

Another favorite saying of ours is "In God we trust; all others bring data."[4] In our Comments, we presented extensive quantitative analysis of robocall complaints to support point (1) above. We posted our dataset (derived from FTC complaint logs merged with other industry databases) so others could confirm or deny our assessment. There were no Reply Comments on this.

With respect to point (3) above, we do not have access to the billions of call records the service providers have, but there have been MILLIONS of calls terminated to our platform. We know which ones are legitimate because once the caller connects, they must enter specific credentials to activate or join a pre-authorized telephonic meeting session.

Scanning recent (legitimate) calls to our platform, we see the following example Caller-ID's:

- 3456, 3488, 9877 (four-digit extensions from a business PBX, lacking the NPA-NXX)
- 317 (area code only; truncated due, most likely, to an inter-carrier misconfiguration)
- 000000000; "missing"; "unavailable" (Caller-ID lost due to legacy interworking)
- 3356130XXXX, 21252243XXXX, 3120555XXXX[5] (international numbers)

[4] Attributed to W. Edwards Demming, a legendary engineer, statistician, professor, author, lecturer, and management consultant.

[5] The actual values in our records contain digits instead of XXXX; the XXXX is used here to protect our customers' privacy. The calls shown originated from France, Morocco, and Netherlands.

We have hundreds of these examples just in the last few days. All of these calls would be deemed blockable under the NPRM; the caller-ID in each case is not a valid NANP number. Microsoft points out in their comments, "It seems unlikely that the Commission intends to allow blocking of nearly all international calls, yet the wording of the proposed rule could do just that since calls from most other parts of the world originate from numbers that are not valid NANP numbers. The public switched telephone network's global reach is one of its strongest features."[6]

The problems leading to these "faulty" Caller-IDs are not going to be readily corrected. While it may be possible to detect SOME truly international calls as such by examining other elements in the call signaling messages, there is no short-term fix that will address all or even most of the existing cases. Similarly, there are doubtless thousands of separate causes for the improper signaling of domestically-originated calls; finding and fixing those, even if there were an appetite to do so, would be a grueling and time-consuming process.

We agree with the VON Coalition: "Call blocking is an extreme response, particularly when blocking standards are not settled and have not been tested for the potential of inadvertent consequences, including with new technologies."[7]

To see just how dangerous this is, consider this from Comcast, one of the larger providers of landline service to American consumers: "Comcast therefore agrees with the proposal to allow blocking of any 'internationally originated call purportedly originated from a NANP number' …."[8] So Comcast would like to prevent any American traveling abroad from calling home with

[6] Comments of Microsoft Corp, page 12.
[7] Comments of the Voice On the Net Coalition, page 2.
[8] Comments of Comcast Corporation, page 21. Available at https://ecfsapi.fcc.gov/file/1070310462677/Comcast%20Comments%20on%20Robocall%20NPRM%20NOI.pdf

their US-based mobile phone. And taken literally, this would block all calls from Canada to the USA. Comcast continues: "The Commission also should consider specifically authorizing voice providers—to the extent feasible as a technical matter—to allow customers to choose to block international calls altogether or on a country-by-country basis, or to *establish a default policy of blocking such calls* unless the customer opts out of such blocking."[9] (emphasis added) I'm flabbergasted that an otherwise-reputable carrier would promote that BY DEFAULT we should isolate Americans from all international callers. That comment should scare the heck out of the Commission. Intended recipients wouldn't even be aware that someone (a traveling family member or friend, foreign acquaintance, or a trusted vendor with an overseas call center) was attempting to reach them.

We mentioned above that many commenters supported the NPRM. How can so many be so wrong? Numerous commenters are outside the industry.[10] They would not be expected to have the technical expertise necessary to evaluate the NPRM, and they do not have access to call signaling data that would let them evaluate the impact of the proposed rules.

There also seems to be see confusion brought about by the invocation of the term "spoof". This term is not well defined (in the NPRM or elsewhere), but if often has nefarious implications. The NPRM says at (5): "Caller ID information can be altered or manipulated, i.e. spoofed" but that is perhaps misleading. Most (but not all) telephone calls contain Caller-ID information and it must come from somewhere. For most conventional phone calls, the originating provider inserts the number of the party initiating the call. When a call is made from

[9] Ibid, page 21.
[10] For example, we did not see any *technical* evaluation in the comments of EPIC, Consumers Union (et al), or 30 State Attorneys General underpinning their general support for the NPRM.

a business telephone system or a call center, that equipment usually generates the Caller-ID information. We generally do not refer to this as spoofing.

When a robocaller places a call, Caller-ID information is part of the call initiation process. The robocaller's equipment includes a value of the robocaller's choosing as the Caller-ID. In the case of a legal robocall, we would expect that value to be a valid telephone number which would identify the robocaller and which, when dialed, would reach the robocaller's office. If these conditions are not met, we consider the number to be spoofed. If they ARE met, then presumably the number is not spoofed.

The NPRM states at (17): "We propose to adopt a rule allowing provider-initiated blocking of calls purportedly originating from numbers that are not valid under the NANP. … *[B]ecause these numbers are not valid, there is no possibility that a subscriber legitimately could be originating calls from such numbers.* Nor do we foresee any reasonable possibility that a caller would spoof such a [invalid] number for any legitimate, lawful purpose; for example, unlike a business spoofing Caller ID on outgoing calls to show its main call-back number, invalid numbers cannot be called back." (emphasis added)

The italicized statement is incorrect. The universe of international numbers comprises one huge example (whether the call is originated outside the US, or by a roamer visiting our country). We have identified other examples above (including calls from business telephone systems that do not or cannot send the complete number). And we have pointed out that as a call progresses from the originating provider via transit providers to the terminating provider, the caller-ID may be unintentionally altered such that it arrives at the call destination appearing to be invalid.

The incorrect statement has misled many commenters into believing that the NPRM is benign when it is not.

But industry commenters should know better. Many hint that the rules could be problematic but support the NPRM nonetheless. We think there are three reasons for this.

First, the rules PERMIT blocking but do not MANDATE it. So even if adopted by the FCC, providers can ignore them without peril. No harm, no foul (another favorite cliché). The NPRM becomes a no-op that providers need not oppose.

Second, industry commenters do not want to offend the organization that also rules on their mergers, spectrum requests, tariffs, and other (more important) regulatory matters.

Third, the Robocall Strike Force erred when it made the request that prompted this rulemaking. Strike Force members are unwilling to admit their mistake.

The NPRM should not be adopted. Adoption provides no benefit and risks blocking of legitimate calls by careless carriers. More importantly, adoption would tarnish the FCC with a misguided rule and would be a disingenuous showing of "progress" in the robocall war when in fact it is not.

There are much more productive places to expend this energy.

NOTICE OF INQUIRY

In our earlier Comments and Reply Comments we emphasized the need for more responsibility on the part of originating providers for keeping illegal robocalls off our PSTN.

We also highlighted the need for better, faster traceback. In their Reply Comments, AT&T indicated: "In AT&T's experience, troubleshooting a call completion issue takes hours or days,

not months. As noted above, AT&T has the appropriate procedures in place to quickly reverse a call block that is affecting legitimate traffic, and AT&T expects that most other carriers have similar procedures, but a carrier cannot address an issue about which it (or, apparently, the service provider of the originating calls) is not aware."[11] While this comment specifically addresses "call completion issues" we believe that AT&T and other carriers have similar ability to efficiently and quickly trace back calls that are identified as illegal robocalls.

We agree with this from AT&T: "AT&T urges the Commission to take steps to encourage—if not compel—all stakeholders to take action to combat illegal robocalls, including through the implementation or modification of procedures to prevent or discourage robocallers from using services for nefarious purposes."[12]

We asked that all providers participate in traceback efforts. We proposed a specific set of things that originating providers can do to proactively limit the ability of their customers to use their services for said nefarious purposes. In his Reply Comments, Vincent Lucas writes: "ZipDX's comment that originating providers should be 'mandated to take responsibility if they won't do it on their own initiative' is interesting, but unfortunately they do not provide any concrete proposals. I would be interested in hearing them elaborate more on this."[13]

In our discussion of a Safe Harbor, we explained that originating providers should be held accountable as end-users if they fail to take such steps. End-users are subject to significant fines

[11] Reply Comments of AT&T, footnote 35 on page 13. Available at https://ecfsapi.fcc.gov/file/107312629008314/7.31.2017%20AT%26T%20Robocall%20Reply%20Comments%20FINAL.pdf
[12] Reply Comments of AT&T at page 13.
[13] Reply Comments of Vincent Lucas at page 5. Available at https://ecfsapi.fcc.gov/file/108012597113018/ReplyCommentsOnAdvancedMethodsEliminateRobocalls.pdf

for each illegal call placed. This would be a strong persuader to otherwise reluctant providers that they should get on board, or face severe liability as demonstrated by the FCC's recent enforcement actions. This is one of the strongest sticks the FCC has.

Some commenters have observed that many robocalls originate from overseas, beyond the jurisdiction of the Commission. We have pointed out that every call on the US PSTN enters through some US provider. An efficient traceback system would enable us to learn who those gateway providers are, and they in turn can work with their overseas partners on mitigation via commercial arrangements. We also know, from examples like the IRS scam which was shut down by the police in India, that overseas authorities are willing to work with us. We need to bring them data, which we can learn via traceback. That is more constructive than a defeatist conclusion that nothing can be done to address internationally-originated illegal robocalls.

We agree with AT&T's promotion of a Safe Harbor that gives providers a measure of latitude to use their best efforts against the illegal robocallers. However, recognizing the risk to legitimate calls when providers are overly aggressive or ill-informed, we believe there should be protections such as those that we suggested in our Comments (including testing blocking rules against historical call data before implementation and playing an explicit announcement to a caller when their call is blocked). That will at least limit the damage should, for example, a provider elect on its own initiative to block all international calls to its subscribers.

We agree with AT&T when they say: "Robocallers are relentless in their pursuit to deceive and defraud American consumers. Indeed, neighbor spoofing is just one example. AT&T identifies hundreds of illegal or highly suspicious robocall campaigns and traffic trends on its network every single day. Just as disturbing, fraudsters and unscrupulous telemarketers constantly adjust their tactics to evade detection and continue their illegal activity. The problem

of illegal and deceptive robocalls thus requires that industry efforts to block such calls be as dynamic and adaptable as the activities of the criminals that providers seek to block. Modifications to existing Commission rules will be needed to afford voice service providers with similar dynamism and adaptability."[14]

The FCC needs to address illegal robocalls via a structure that is dynamic and responsive (which the NPRM/NOI process is not). We have suggested a Robocall Czar that would aggressively lead a cooperative industry effort (evolved, perhaps, from the Strike Force, with more focus on the items in this proceeding, structured as on on-going iterative effort, and committed to critical thinking and data sharing) to address this challenge. The Commission should quickly explore (with industry and other experts) how best to move forward with that.

Respectfully submitted,

DATED: August 4, 2017

/s/ David Frankel

dfrankel@zipdx.com
Tel: 800-372-6535

[14] Reply Comments of AT&T at page 6.